Req. # 3871

T1500M/IF 175

Reel #3

SEABOURNE REPORT
VOL. XIII

CRYPTANALYSIS

THE SIGNAL INTELLIGENCE SERVICE
OF THE
GERMAN LUFTWAFFE

VOL. XIII

CRYPTANALYSIS WITHIN THE
LUFTWAFFE SIS

VOL. XIII

CRYPTANALYSIS WITHIN THE LUFTWAFFE SIS

F O R E W O R D

Firstly, there is contained in this volume certain studies prepared by Ferdinand Voegele and Lieut. Berthold Pick, who served as chief and assistant chief, respectively, of Referat E of the Chi-Stelle throughout the course of World War II. This Referat of the Chi-Stelle, central SIS bureau of the Air Ministry, it was that dealt with a study of enemy cryptographic systems incapable of solution in the field.

Included also is a study in the original German text, which discusses the cryptographic systems employed during the war by the air forces of the Soviet Union. This study was submitted by Lieut. Waldemar Werther, cryptanalyst of the 353rd Regiment, East, Luftwaffe SIS, whose biography is to be found in Vol. II.

Translation of Lieut. Werther's study was not undertaken by members of the Air Technical Intelligence Team, USAAF, since time was lacking in which to do it justice. Then too its subject matter is quite technical and believed to be of interest, in the main, to cryptanalytic specialists only.

J.G. SEABOURNE
Colonel, Air Corps
SIS, USAAF.

VOL. XIII

CRYPTANALYSIS WITHIN THE LUFTWAFFE SIS

TABLE OF CONTENTS

TOP SECRET

CAREER IN THE SIS

OF

Ferdinand Voegele
Chief, Referat E, Chi-Stelle
Luftwaffe SIS.

I was born on the 12th of February 1896 in Hollfeld, Bavaria. I served in World War I as a volunteer, following which I studied oriental languages at various universities, specializing in philology. I also engaged in the export business. After several years of residence abroad, I was offered a position as interpreter, in the summer of 1935, with the German Air Ministry.

1935 July to September: Training at Kladow, near Berlin, in Morse telegraphy, German cryptographic procedures and radio communication in general.

October to January (1936): Transferred to the fixed SIS station of the Army at Stuttgart. There I translated plain-language radio messages from the French, partly Army, partly Air Force, and in addition was employed on evaluation and traffic analysis.

1936 March to April: Ordered to a two-months' maneuver, where I was employed as an airborne radio operator with KG 254 at Kitzingen, on the Main. My grade was that of officer candidate.

May to October 15th: I broke the recipherment used in connection with a French Army 3-figure code, the basic book of which had, for the most part, already been reconstructed. The recipherment was done with a number-letter cipher table, which changed at irregular intervals. After the outbreak of the Spanish civil war, I solved many Spanish four-alphabetic substitution ciphers.

October 15th: I was transferred to a newly-activated Luftwaffe intercept station (W-15) in Munich/Stadelheim, where I translated French, Italian, and Jugoslavian radio messages. I could not engage in my real work, which was the deciphering of Czechoslovakian messages, since such messages were not intercepted at this time.

1937 On the first of January, I was ordered to the newly-created Chi-Stelle of the German Air Ministry, and was assigned to Referat E, under Captain Imdisch. I was made chief of all cryptanalytic work. The entire Chi-Stelle consisted of about a dozen people. An assistant by the name of von Lingen was assigned to me, who had learned the cryptanalysis of Russian Army traffic at a German Army SIS station in Treuenbrietzen. The Russians had no independent air force, and accordingly no special air force radio procedures.

During the remainder of this year, I broke other Spanish systems, and several Czechoslovakian bigraphic procedures. The material available for breaking the Czechoslovakian Air Force double-transposition cipher amounted to only 10-25 messages per day.

1938 The deciphering of Russian traffic, for which more people were available than for all other countries combined, presented no new problems in this year, nor in the following years. The systems were 2-figure and 3-figure simple substitution ciphers, as well as a 5000 group code book, changes in which presented no great difficulties, since the position of the individual code groups in the revised editions remained relatively the same. The recipherment was always perfomed with a 2-letter substitution table. Since the cryptanalytic work on Russia was the specialty of Lieuts. von Lingen and Werther, I can add no more pertinent details.

In this same year, several Czechoslovakian systems, bigrams, training codes, simple transposition, and, in the summer, also double transposition ciphers were solved, as well as several Slovakian substitution ciphers. The double transposition ciphers were all based on keywords beginning with the letters "A" or "C".

The amount of Polish traffic intercepted during 1938 and 1939 was very meagre. The number of messages, enciphered in the principal Polish system, which was a 4-figure code, reciphered with an additive, only reached a total of 100 in one particular month. During 1939, the average number of messages intercepted was well under 100 per month, making cryptanalysis impossible. In September, 1939, the code book was captured, but less than 10 messages were transmitted during the month. Simple substitution ciphers were broken in 1938-1939.

Owing to a shortage of personnel, only one cryptographic system of the Western Powers, namely, a French Air Force system, was worked on in the fall of 1938. This was a 4-letter alphabetical code book, reciphered with a mixed number-letter cipher table. The average depth of messages was 100 per month, and in the spring of 1939, the first message was read. British, Dutch, Belgian or American systems were not studied.

1939 An average of ten people only were available for cryptanalytic work. A Jugoslavian 4-figure alphabetic code with three different types of reciphering was worked on. In spite of changes, the reading of this traffic continued during 1940.

Further reconstruction work was done on the French Air Force code book. In about May, 1939, the first groups of the Government Telegraph Code were

identified, in connection with the analysis of the RAF 4-figure system, which I had labelled as decipherable, though no one agreed with me. Some Syko messages were intercepted, from which it could only be decided that a thirty-two column substitution table was being used. At the outbreak of the war, I had available for cryptanalytic work on the traffic of the Western Powers only four men, none of whom could be classified as a good cryptanalyst. All these people were later eliminated from the Referat. After submitting a report, stating that under the prevailing personnel policy no results could be produced, about fifty Signal Corps enlisted men were assigned to me by General Martini, the Luftwaffe Chief Signal Officer. These were mostly young people, some of whom had studied languages in school, all of whom possessed no knowledge or experience in the field of cryptanalysis. There was no time for training, so I immediately set these people to practical work. Several weeks later, the first hundred groups of the 4-figure code book were identified.

In the case of Syko, the average depth of traffic at the end of 1939 was 15-20 messages per day, with the result that deciphering was impossible; this in spite of the fact that the Syko cards for the entire month of October were recovered from a Wellington shot down near Gotha on the 2nd or 3rd of the month. Only at the beginning of 1940 did the increased depth of traffic permit the deciphering of Syko messages.

Of the French systems, those messages encoded in a 4-figure system, reciphered with letters, were intercepted in small quantity only until the end of 1939. These messages could be read, but at the end of the year this traffi ceased. Other French systems were not intercepted.

By September, 1939, the total cryptanalytic personnel available for work on all countries, including Russia, was 15-18 in number. By the end of December it had risen to 50.

1940 Work on the RAF 4-figure code continued, the deciphering work being done by the Chi-Stelle in Potsdam, W-Leit 2, W-12 in Brussels, and by W-Leit 3 in Bougival.

In January and February, Syko messages were deciphered with a depth of traffic of up to 300 messages a day. Many cards were completely reconstructed, and when at our best, the messages were read by 1400 hours the same day. Of special value were the numerous weather messages encountered in this traffic. Syko traffic was analyzed primarily by the fixed SIS station in Husum, but also in Brussels and Paris.

The period, March to April, saw the breaking of the British 5-figure weather system, reciphered with an additive, in much the same way as the RAF 4-figure code. After the system was broken, it had to be turned over to the Chief Weather Officer, but, in the case of a change in the additive book, the Referat was again allowed the honor of performing this work.

During March and April, a Belgian 3-figure procedure, and a Dutch bigraphic system were broken.

In June work was begun on the Inter-Departmental Cipher (British). For this purpose not only a copy of the code book was available, but also a great number of radio messages, which were intercepted by the Dutch and Norwegian Signal Intelligence Services. The only work done by the Dutch and the Norwegians had been to arrange the cipher text with five groups to

a line. By exchanging cipher texts with the Chi-Stellen of the Army, Navy and Foreign Office, this system was read continuously.

In the late summer of 1940, the greater part of the Referat was moved to W-Leit 3 in Paris, where for several months, optimum results with the RAF 4-figure code, Syko and IDC were attained. By means of the 4-figure code and IDC, several additive books were completely reconstructed.

At the end of 1940, a cryptanalysis team for RAF 4-figure code was sent to Taormina in Sicily to join the 9th Company of LNR 40, commanded by Captain Windels (later Major). This team likewise achieved very good results.

1941 January and February brought no change. However, another cryptanalytic unit, of approximately 12 men, to work on the RAF 4-figure code, was sent to the Balkans to the 8th Company of LNR 34 (Captain Boehme) with Fliegerkorps VIII. This unit also functioned efficiently until the introduction of the new edition of the 4-figure code on the first of April.

Despite my remonstrances, my cryptanalysis unit was ordered in March to leave W-Leit 3 and join Referat B at Asnieres. Poorer intercept conditions, coupled with many fewer and less experienced radio operators brought a general deterioration. Nevertheless the new RAF 4-figure system was quickly broken.

In May, the greater part of my unit in the West was transferred to Athens, and there achieved very good results with the 4-figure code and other systems from the fall of 1941 to the fall of 1942.

That portion of the unit which remained with Referat B in Asnieres, worked primarily on IDC. These people, who were specialists on this system, could

decipher much of the traffic with a relatively small number of messages.

In November, Luftwaffe SIS units in Norway intercepted the first American 5-letter messages, enciphered in a strip system, and containing the indicator, "URSAL". However, the interception of this traffic was dropped a few days later.

As ordered, the cryptanalysis team with Referat B in Asnieres continued to work on the RAF 4-figure traffic, but the number of messages (about 60 per day) was much too small, and moreover so poorly intercepted, that this work could bring no results.

The war with Russia, although it brought an increase in interception, revealed no new systems. The Russian 5-figure system, reciphered with an additive, was broken as early as the summer of 1940. Copies of this alphabetical code were captured in 1941 and 1942. The bulk of cryptanalytic work on Russian traffic was done in the Marstall at Potsdam until the late fall of 1941; then in Niedersee (East Prussia); in May 1942 it was done at Zitomir, Russia, in 1943 in Goldap, East Prussia; all corresponding to the movements of the Chi-Stelle Headquarters.

1942 In January, the cryptanalysis team with Referat B at Asnieres, was ordered back to the Marstall, but it was March before it arrived there. The reason for this delay was the interception of American cipher messages. In April, a small number of "URSAL" messages were intercepted allowing the system to be broken. Moreover, it was discovered that the same system, with the same strips, was accurately described in a pamphlet which could be bought for thirty cents, the title of which, as my memory best serves me, was, "The Field Officer's Manual".

With the help of a small IBM (Hollerith) unit, work on the strip system used on the South Atlantic ferry route was begun in the fall of 1942. Messages intercepted during May, bearing the indicator, "CENEB", were used as material. With a maximum depth of traffic of 250 messages per day it was possible to reconstruct the 100 strips. In January, 1943, traffic of the months succeeding May, 1942, was almost completely deciphered. The maximum success achieved was the decipherment of the messages 14 days after interception. This work was done only in the Marstall, the interception being accomplished by the 15th Company of LNR 3 in Munich/Oberhaching, and by an intercept platoon with Referat B in Asnieres. The IBM machines, which were absolutely necessary for finding repetitions in messages, were located in Treuburg, and later Berlinchen, both in East Prussia, which fact occasioned great delay.

At W-Leit, Southeast, in Athens, excellent results were obtained, during the summer and fall of 1942, with the British 4-figure traffic, and the weather code; to a lesser extent also with Mediterranean Syko and IDC. The cryptanalytic group in Athens was increased to 140 men, most of whom were used on British systems including the Aircraft Movement Code, which was identified there in the fall of 1942. A small number of these people sufficed to decipher the transposed Turkish weather cipher. The deciphering of the Turkish simple substitution cipher, which changed monthly, offered no great difficulty. The Turkish number code also presented no particular problem.

At the end of 1942, the American cryptographic system of the Caribbean Defense Air Force (indicator "CDAF") was also read. Two-digit numbers, in this system, in addition to being encoded, were reciphered with a small additive table. These messages contained reports of take-off.

At approximately the same time the first attempts were made to decod Bomber Code messages. Owing to the slight depth of traffic, this was no possible even though several captured copies of the code were available.

Since I myself had personally twice broken the RAF 4-figure code, I assumed that the new system, which went into effect on the first of Nove could be broken by W-Leit, Southeast, in Athens. Moreover, I was at thi time primarily occupied with the American strip system, as well as the B Code, Aircraft Reporting Code (which was still unbroken), Division Field etc.

1943 In the beginning of January, the first partial decipherment of the B Code was achieved. To further this work, I sent a small team to Meldeko in Zeist, Holland. The depth of this traffic gradually increased, and i daily decipherment was possible until the end of the war.

In February, we succeeded in breaking Division Field Code messages i Mediterranean theatre, most of which contained air force strength report memory serves, sufficient messages, encoded in DFC-17, DFC-19 and DFC-21 sent on American Air Force networks to permit their being read in part.

About this time the enlisted men who were employed as cryptanalysts to be replaced by women auxiliaries. In March and April, RAF 4-figure intercepted in Athens was sent to the Marstall, and at the same time the cryptanalytic personnel in Athens was recalled. Research work was done this system with the help of IBM machines, but only insignificant and p results were obtained.

the code book would be changed at shorter intervals, the fear that the cryptanalytic successes of W-Leit, Southeast, in Athens might be divulged by a deserter from this unit, and, finally, the pressure of other, more urgent cryptanalytic work, all led to the fact that this system was given only a minimum of attention, with very little success ensuing. In the spring of 1944, the interception of RAF 4-figure messages was abandoned entirely.

Meanwhile, the number of messages intercepted in the American strip system used on the South Atlantic route, was sharply reduced, the greatest number of messages intercepted in any one day being only 150. Difficulties were further increased by the removal of five of the thirty strips, which five could be removed at random with each message. Individual messages were deciphered, but the results did not warrant the expenditure incurred in time and labor. By the beginning of 1944, the maximum number of messages with the same main indicator, intercepted in one day, had fallen to 100 and the average was 50. Thus further analysis was rendered impossible.

Toward the end of 1943, the first attempts were made to break the M-209. Nevertheless, since a much greater number of these messages were intercepted by the Army SIS (for a while ten times as many), analysis was at first impossible without an exchange of messages with the Army. The Army SIS remained the leader in the interception of these messages, and, therefore, the leader also in their decipherment.

During this year, and also in the following years, various attempts were made to render feasible the decipherment of Mediterranean Rekoh cards. In 1943 and 1944, a string of Rekoh cards were reconstructed; but since it was never possible to devote sufficient radio receivers to the interception

of these messages at any one station, the deciphering, which under these conditions depended on the relaying of them from three or more intercept stations, could only be accomplished after a delay of several days, in which case it had no great significance.

No important changes took place in the analysis of Russian and Turkish traffic.

1944 During maneuvers in England bigram messages were transmitted, which could be partially deciphered. This proved to be the Slidex system, which afterwards was used in the Invasion, and by that time had been in the greater part reconstructed.

The Anzio landing in Italy produced a simple, new bigraphic system. Frequently these messages contained requests that the answers to specific questions be enciphered by means of M 209.

In February, the interception of Aircraft Reporting Code messages by the 16th Company of LNR 3 in Angers increased so sharply that partial deciphering was possible with a depth of 150 messages per day. From July, 1944 on, work on this traffic was transferred to the fixed SIS station in Husum.

In March, the first M-209 messages on American Air Force networks in the Mediterranean were deciphered.

Since November, 1943, about 150 5-letter messages, with the indicator "TELWA", had been intercepted. These proved to be an unenciphered code. An average of four men worked on this system. Since the code was an alphabetic

one, more than 10,000 groups of the code were accurately identified, although only approximately 1000 messages were available up to March, 1945.

In the fall of 1942, the Aircraft Movement Code had been broken for the first time, and thenceforth was currently read. Various difficulties such as the use of two codes, one American and one British, twelve-hourly changes, the introduction of many variants, etc., made the deciphering task increasingly difficult. During the summer of 1944, several attempts were made to solve the problem with IBM machines, but with no success. Even the messages sent on American high-speed radio teletype links, which messages contained ETA and ETD information, as well as details on markings of the aircraft, proved no point of entry for the decipherment of the Aircraft Movement Code messages which, from this time on, was no longer possible.

As of the day of the Invasion, the 6th of June, the following systems were being read: Bomber Code, Aircraft Reporting Code (to a limited extent; analysis was facilitated by weather messages), Slidex, and, on certain days of the month, M-209 and "TELWA".

This situation remained undisturbed for the remainder of the year. Toward the end of the year, M-209 messages on MAAF networks were deciphered more frequently. In October, 1944, it was possible to decipher the entire traffic of a network in the West for four weeks by virtue of a captured list of M-209 settings.

1945 With the passing of 1944, German signal communication continually deteriorated. Individual units were moved about more frequently, Referat E, itself, being transferred to Kressbronn on the Bodensee, in February. Thus it came about, that cryptanalysis teams with individual units were cut off,

and the Referat, itself, received no more messages from outside sources. The IBM installation was overrun by Russian troops at the end of January; a new one was procured, and was operational by the end of April, but individual headquarters were disintegrating on all sides.

I, myself, during the war, made about one hundred trips in the interest of the service, always to those places where new difficulties had arisen. Until May, 1943, although responsible for cryptanalysis in both the West and in the Mediterranean theatre, I had no officer or inspector in my Referat, and in addition to visiting Luftwaffe SIS out-stations, I had to undertake liaison with the other cryptanalytic organizations of the Wehrmacht myself.

During the month of January, 1945, 15,000 Russian messages were deciphered and 35,000 of the Allies in the West (including the Mediterranean).

REVIEW OF AMERICAN CRYPTOGRAPHIC SYSTEMS

By

Ferdinand Voegele,
Chief, Referat E, Chi-Stelle
Luftwaffe SIS.

1. "URSAL" and "CDAF"

These two systems, one of which was used on the North Atlantic ferry route, the other in the Caribbean Sea area, were worked on and broken during 1942-1943.

Out of fifty strips, twenty-five were selected for any single day and were used in prescribed sequence. The twenty-five letters of the alphabet were read fr one column according to the de Baseries method. After approximately forty of the strips had been reconstructed, a short repetition in two messages sufficed to permit the arrangement of the strips to be determined.

2. Five-Figure Procedure

Two code tables of 100 groups each formed the basis of this procedure, which was solved in 1942-1943. One of these tables contained the letters of the alphabe numbers, symbols, etc., the other such frequently used words as ETA, no, from, lef etc.

Only two-digit numbers were reciphered from a small additive table; other code groups were not reciphered. The result was that one message usually sufficed to break the recipherment. The contents dealt with air-to-ground traffic, and the number of messages intercepted was limited.

3. Thirty-Strip Procedure on the South Atlantic Ferry Route

The first messages analyzed in this system were those of the month of May, 1942, bearing the indicator "CEMKB". It was quite evident from the cipher text that there was a break after each fifteen letters, indicating that another strip was being used. Accordingly an analysis was made on the basis of groups of fifteen letters with the assistance of IBM machines. A depth of 80 passages of parallel construction was needed to reconstruct the 100 strips, 30 of which were valid in any one day.

In order to make cryptanalysis possible, a minimum of 150 messages was needed on most days of the month. More than this number was usually intercepted. The system was used for air-to-ground messages on the South Atlantic ferry route, and was read as long as it was used.

In 1943 a new difficulty presented itself. While 30 strips were still valid on any one day, the encipherer could arbitrarily remove any five of the strips to encipher any one message. To indicate which five had been removed, a second indicator group, probably referring to a small chart, was used. After about six weeks, some of these messages were also deciphered. However, at the same time the volume of this type of traffic began to decline, so that finally the analysis work had to be discontinued. In this system the two indicator groups were repeated in inverted order at the end of the message.

Another cryptographic system was used for this same type of traffic. Again two indicators were used, the first of which was usually an alternate consonant-vowel combination (e.g."BACED"), the second, of no particular pattern. Both indicators were repeated in the same order at the end of the message. It was probably a machine cipher, but not the M-209. Detailed research was not possible, owing to the replacement of male cryptanalysts with inexperienced female auxiliaries.

4. Bomber Code and Rekoh (See British Systems)

In order to become familiar with the contents of Rekoh card messages, which were used by the Americans on the Atlantic ferry route, one day's traffic, which was especially favorable, and consisted of about sixty messages, was deciphered in mid-March, 1944 by the 16th company of LNR 3 in Angers. The evaluation section was not especially interested in the contents of these messages; therefore work on them was stopped.

5. Division Field Code

A copy of this code (to the best of memory, edition DFC-17) was captured in the Mediterranean area. Because of this, it was possible to partially decode the small number of intercepted messages which had been encoded in other editions such as DFC-19, 23, 28 and 29.

6. Aircraft Movement Code

As with its British counterpart, this system was introduced at a relatively late date, and was found by the German SIS to be identical with the British system. It was used for ferry flights over the Atlantic and the west coast of Africa. Even when the system could no longer be deciphered because of frequent changes, the approximate number of aircraft being ferried could still be determined by the evaluation section from the depth and numbers of groups of the messages, as well as the time of day at which they were sent.

7. M-209

This was a 5-letter system with the two indicator groups repeated at the end of the message in the same sequence. The first six letters indicated the setting of the machine, which had been used for that particular message. From these the real indicator could be obtained by repeatedly enciphering a double letter given in the

eleventh and twelfth groups of the external indicator. The ninth and tenth letters indicated the organizational system (i.e. 15th USAAF, 9th USAAF, etc.). Sometimes the information contained in the indicator groups was arranged in a slightly different order (e.g. the double letter might occur as the first and second letter of the first indicator group, etc.).

To derive the actual machine setting so that messages of one day in the same system could be deciphered, either two compromised messages (where a part of the plain-text could be assumed and superimposed) were sufficient, or one message with mistakes, which was later correctly re-enciphered in the same system and key. In these two cases the deciphering of 50-60 letters had to be accomplished in order to obtain the setting valid for a twelve-hour period. The average depth of traffic in the West was 100 messages per day; in the Mediterranean, 40. Two or three systems used in the West were read on between six to twelve days of each month, while in the Mediterranean the average was two to five days.

In the most successful cases an entire system was broken in 24 hours. In general, however, better results would have been obtained, had the interception of these messages been more purposefully directed.

8. TKLWA

This was a 5-letter system, which was intercepted by the Luftwaffe SIS from November, 1943 on. It was based on a code book of approximately 130,000 to 140,000 groups, and was not reciphered. Since the code book was arranged in alphabetical order, more than 10,000 groups had been identified by April, 1945. This number sufficed to read practically all well-intercepted messages, insofar as their contents did not involve an unusual vocabulary. The number of these messages intercepted by all three branches of the Wehrmacht aggregated less than 100 per month.

The system was frequently used by air attaches and liaison officers especially in Sweden and the Near East.

REVIEW OF BRITISH CRYPTOGRAPHIC SYSTEMS

By

Lieut. Berthold Pick,
Referat E, Chi-Stelle,
Luftwaffe SIS.

1. Government Telegraphic Code

Work upon this code was begun by the Chi-Stelle of the Wehrmacht in May, 1939, it being at the time unknown to the Chi-Stelle of the Luftwaffe, even though it was not secret. In August, 1939, the code was turned over to the Luftwaffe by the Wehrmacht. It was used to encode reports of casualties, and for administrative messages. On the 28th of August 1939, the Admiralty in London broadcast an encoded "CQ" message, which read: "All ships home".

The average depth of traffic in this system was 200 messages per month. Less value was attached to this code in the latter years of the war.

2. India Code

Work on this 4-letter code, which was transmitted in 5-letter groups, was begun in 1939-1940 by Referat E, and was partially read until the end of the war, with a small depth of traffic. The code group "TAFA" meant "begin spelling".

3. Syko Cards.

The Syko card was used to recipher messages encoded with the Royal Air Force Naval Code. A copy of this code was retrieved, in the beginning of September 1939, from a Wellington shot down in an attack on Wilhelmshaven. This code, with few deviations, remained in effect until the end of the war.

Work on deciphering the Syko card was begun in January, 1940, by the fixed SIS station in Husum. By February 1940, the Syko card was being reconstructed almost daily, and could be read by 1600 or 1700 hours. Later, several cards rather than one were used daily. Nevertheless, the individual cards could be reconstructed with a depth of 40 messages.

RAF messages concerning both British and Axis naval vessels, submarines, convoys, etc., were of special interest. Messages of commercial air lines (indicators GEM, GER, etc.) gave a complete picture of the weather situation.

Depth of traffic ran to between 80 and 300 messages per day.

4. Rekoh Cards

This card appeared in 1942-1943 in place of the Syko card. Since it was not constructed reciprocally, its reconstruction proved somewhat more difficult, but was accomplished by virtue of the previously attained experience with Syko, only a slightly increased depth of traffic being required.

5. RAF Four-Figure Code

This code was divided into two parts, was not arranged alphabetically, and was reciphered with an additive. The system was broken in two stages:

a. Removing the recipherment.

b. Decoding the original groups thus revealed.

Certain groups of the basic code were already known. By comparing those messages reciphered with the same set of additives, it was possible to superimpose certain stereotyped words or phrases (internal addresses, delivery groups, parentheses, etc) where repetitions in the cipher text occurred. By subtracting the basic 4-

figure code groups from the cipher groups, the additives were then obtained, and, moreover, when taken in relation with the indicator group, sections of the additive book itself could be slowly reconstructed. Reconstruction of the original code book was greatly facilitated by the fact that on the 24th and 31st of December, 1939, encoded messages were transmitted without being reciphered.

If the additive had been determined, even unknown code groups could be identified on a frequency basis, by their position in the text, and through the use of "spellers".

By March, 1940, it was possible to read these messages in part, and from then on with increasing success. The additive books used were later changed every three to seven days. Within the course of the effective period, many of them were almost completely reconstructed.

On the 1st of April 1941, the basic code book was changed; but, in spite of a dearth of traffic, was being read four weeks later. Until November, 1942, the majority of messages were read by W-Leit, Southeast, within two to fourteen days of their interception.

On the 1st of November, 1942, the code book was once more changed. From then on only fragments of messages were read.

The procedure was used in England, and later in the Middle East primarily. During the winter of 1941-1942, messages averaged as high as 600 per day. This figure gradually dwindled, until in early 1944 they averaged less than 100 per day, and by the summer of 1944, interception of them was discontinued altogether.

6. Inter-Departmental Cipher (IDC)

This also was a reciphered 4-figure code. The code book was captured in Bergen during the occupation of Norway, and a photostatic copy furnished to Referat E. Work on the reciphernent was begun in June, 1940, and by July of the same year the first messages were being read.

The system was used by air attaches, and the majority of messages could be read with a depth of about 300 per month.

Since the evaluation section was no longer interested in the contents of these messages and the interception of them had been sharply reduced, cryptanalytic work on them was abandoned in the spring of 1942.

7. Bentley Code

In the summer of 1942, approximately 300 special groups (those beginning with "Y", which were a special war-time addition) of the Bentley code (commercial) were identified. In the winter of 1942-1943 the code was reciphered with a 5-figure additive. Only small portions of the additive book were reconstructed. It was used by the British Airways in South Africa, Southeast Africa, Egypt and Syria.

Messages were intercepted at the rate of ten a day.

8. Aircraft Movement Code (AMC)

In the fall of 1942, work on the solution of the Aircraft Movement Code was begun by W-Leit, Southeast, in Athens. The system comprised pronounceable 5-letter code words, which were changed every twenty-four hours. In 1943 a system of two settings daily was introduced, still changed every twenty-four hours. Later both settings were changed every twelve hours.

It was used for ferry flights from Takoradi to India, via Maiduguri and Egypt. The depth of traffic was up to 500 messages daily.

From February 1944 on, the code could no longer be read because of the introduction of too many variants.

9. Bomber Code

The first Bomber Code messages were intercepted in November, 1942, and from January, 1943 until the end of the war, were currently read by Meldekopf 1 in Zeist Holland. The code was used by the British and Americans jointly, to the disadvantage of the British. It was changed daily at 0300 hours. Therefore, if an American raid took place during the day, the code would be broken in time to permit messages of the RAF night bombers to be read immediately. The depth of messages averaged 300 per day, sometimes running over 300.

10. Aircraft Reporting Code.

The Aircraft Reporting Code was used by reconnaissance aircraft in the West from July, 1943, on, replacing Syko and Rekoh. It was first broken in February, 1944, by the 16th Company of LNR 3 in Angers. Later, owing to a lack of intercepted messages, the code was only partially read in connection with the UCO Code (weather) by the fixed SIS station in Husum.

11. UCO Code

The UCO Weather Code was partially broken in May, 1944, by the 16th Company of LNR 3 in connection with the Aircraft Reporting Code. Primarily barometric pressure, given in 7-letter groups, was deciphered. From July, 1944, on, the UCO Code was worked on in Husum. The depth of traffic was up to 300 messages per day.

12. Slidex

In the middle of May, 1943, work on Slidex was begun by the 3rd Battalion of SIS Regiment, West, in Bougival, near Paris. It was a bigram system, reciphered with 5-letter cipher strips which changed daily. Slidex messages were read in entirety ever since the Invasion. The cipher strips were reconstructed each day by 0700 to 0900 hours. The average depth of traffic per strip was 15-40 messages per day.

13. Air Support Party Networks in Italy

In 1944-1945 short messages were transmitted on ASP networks in Italy, containing one of the words "Sweet", "Sugar", or "Candy". For a while, tune, and number of aircraft requested could be quite accurately determined from them. When the cipher key was changed hourly, or every two hours, a definite identification was no longer possible.

14. Weather Codes.

a. From February to April, 1940, the Main Weather Code (5-figure with 5-letter indicator) was broken by the Chi-Stelle, and after solution was turned over to the Signal Weather Monitoring Station (WENUEB) at Glindow, near Potsdam.

b. In April, 1942, W-Leit, Southeast, worked on a 5-figure Middle East weather code, and upon its solution turned it over to WENUEB.

c. The principal weather codes used in the Atlantic area, bearing the indicator "Whist" and Tooth", were worked upon by WENUEB. To the best of the knowledge of Referat E, this effort met with no success.

d. The deciphering of weather messages, insofar as they could be externally recognized as such, was not the function of Referat E, but rather of WENUEB, the

central weather bureau at Glindow. The Referat acted only in an auxiliary capacity.

15. Miscellaneous Systems

a. Transposition Cipher: There were several systems of this nature used in the various theatres of war, which could be deciphered.

In Great Britain itself, a transposition cipher, involving a rectangle ten columns wide, was used. This system was changed every Thursday at 2400 hours by transmitting the new key word, enciphered in the previous system.

b. Double Transposition Cipher: In spite of notebooks captured during the reconquest of Leros, and data found during the first stage of the Normandy Invasion, this system could not be broken, owing to a lack of sufficient messages in the same key, and of the same length.

c. Typex

In the summer of 1940, attempts were made to break this machine cipher. It was soon realized, however, that these efforts were of no avail.

LIAISON AND CO-OPERATION BETWEEN THE LUFTWAFFE CHI-STELLE AND OTHER CRYPTANALYTIC CENTERS

By

Ferdinand Voegele
Chief, Referat B, Chi-Stelle
Luftwaffe SIS.

During 1937 and 1938, liaison with the Chi-Stelle of the Wehrmacht was limited to an exchange of identified code groups within the Russian code book. The Czechoslovakian double-transposition cipher was being worked on by the Wehrmacht Chi-Stelle, but it had not been broken.

In the spring of 1939, the Wehrmacht was interested in the French Air Force 4-figure code, reciphered with letters, which I had broken. I forthwith supplied them with those code groups which had been identified, and an explanation of the recipherment.

My first liaison contact with the Chi-Stelle of the Navy took place in 1939. My object was the request that the Navy pass over to us, copies of RAF 4-figure messages that they were intercepting, to which request they acceded. We also discussed the question of Syko messages, the decision being that the cryptanalytic work on this system should remain with the Luftwaffe, and that Syko messages intercepted by SIS units of the Navy would be passed by teletype to the cryptanalytic platoon with the fixed SIS station in Husum, to which station a naval liaison officer was later permanently assigned.

At the turn of the year, first contact was made with the Chief Weather Officer, and the promise given that the weather codes, mostly British, would be furnished to him as soon as they were solved.

In the spring of 1940, a lieutenant-commander of the Italian Naval Ministry, visited me, and at his wish I explained to him the method used in deciphering Syko.

In the summer of 1940, a gentleman of the Wehrmacht came to my Referat at Potsdam, and there received instruction on breaking the additive used with the Inter-Departmental Cipher(British). Messages in this system, intercepted by the SIS organization of the Wehrmacht, the Navy and the Foreign Office were furnished to the Luftwaffe Chi-Stelle, and while work on this system lasted, newly identified additives were likewise exchanged. Eighty percent of the additives were reconstructed by Referat E.

In the beginning of 1941, a central liaison office was established in the Air Ministry which arranged for the exchange of messages and additives between the several Chi-Stellen, including, in part, that of the Foreign Office.

In February, 1942, through the auspices of the Wehrmacht Chi-Stelle, I sought to establish contact with a Japanese, Colonel Hajashi, who was at that time in Berlin. However, nothing came of this attempt, as I was continually put off by Colonel Kempf, the chief of the Wehrmacht Chi-Stelle, who did not approve of this idea.

At about this time, I sent five people to the Italian Naval Ministry, in Rome, to work there on RAF 4-figure messages, principally because these messages were being intercepted in Monterotondo and elsewhere in Italy. No other cryptographic systems were exchanged with the Italians. Meetings which I had with General Gamba, and officers of the Italian Air Force were without significance.

In 1942 and 1943, messages, and, in part results, were exchanged with the Army Chi-Stelle in Berlin relative to certain American systems, among which were "URSAL", "CDAP" and the Division Field Code. Since our own IBM installation in the Marstall was incomplete, several joint research experiments were conducted at the Reichssportfeld (National Athletic Stadium in Berlin) where the Hollerith company had made available a complete installation in one of the larger halls.

The American cipher strip system used on the South Atlantic ferry route was broken in my Referat. It was also used in American diplomatic traffic, and my method of solution was adopted by the Chi-Stellen of the Wehrmacht and Foreign Office.

During the years 1943-1945, M-209 messages and results were exchanged with the Army Chi-Stelle, NAAST 5 (Army SIS center in the West), and the Navy Chi-Stelle. Army out-stations intercepted many more M-209 messages than did those of the Luftwaffe; of the three services, the Navy intercepted by far the least.

During the second half of 1944, and until March of 1945, "TELWA" messages were exchanged between Referat E and the Chi-Stelle of the Wehrmacht. Newly identified code groups were exchanged with both the Wehrmacht and the Army.

During the period shortly before the Invasion, and for as long as they were not separated by too great distances, close co-operation existed in the fields of Slidex and M-209 between NAAST 5, and those companies of SIS Regiment, West, to which cryptanalytic teams were attached.

Throughout the entire war I enjoyed close association with the leading figures engaged in cryptanalytic work, and by means of these contacts views and experience were exchanged. In general, regular liaison officers were not maintained.